PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 :		(11) Internationale Veröffentlichungsnummer: WO 99/22486
H04L 9/32	A1	(43) Internationales Veröffentlichungsdatum: 6. Mai 1999 (06.05.99)

(21) Internationales Aktenzeichen: PCT/EP98/06769

(22) Internationales Anmeldedatum: 24. Oktober 1998 (24.10.98)

(30) Prioritätsdaten:
197 47 603.1 28. Oktober 1997 (28.10.97) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: BROKAT INFOSYSTEMS AG [DE/DE]; Industriestrasse 3, D–70565 Stuttgart (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: RÖVER, Stefan [DE/DE]; Ulmenstrasse 20/1, D–71088 Holzgerlingen (DE). GROFFMANN, Hans–Dieter [DE/DE]; Birkenstrasse 14, D–72145 Hirrlingen (DE).

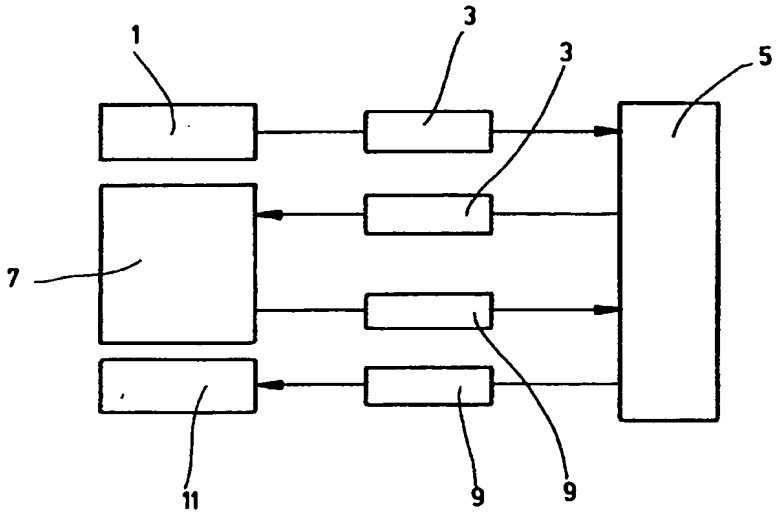
(74) Anwälte: SCHRELL, Andreas usw.; Maybachstrasse 6A, D–70469 Stuttgart (DE).

(81) Bestimmungsstaaten: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO Patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht
Mit internationalem Recherchenbericht.
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(54) Title: METHOD FOR DIGITAL SIGNING OF A MESSAGE

(54) Bezeichnung: VERFAHREN ZUM DIGITALEN SIGNIEREN EINER NACHRICHT



(57) Abstract

The invention relates to a method and to the necessary means for digital signing of a message.

(57) Zusammenfassung

Die Erfindung betrifft ein Verfahren zum digitalen Signieren einer Nachricht sowie die dazu notwendigen Mittel.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	**ES**	Spanien	**LS**	Lesotho	**SI**	Slowenien
AM	Armenien	**FI**	Finnland	**LT**	Litauen	**SK**	Slowakei
AT	Österreich	**FR**	Frankreich	**LU**	Luxemburg	**SN**	Senegal
AU	Australien	**GA**	Gabun	**LV**	Lettland	**SZ**	Swasiland
AZ	Aserbaidschan	**GB**	Vereinigtes Königreich	**MC**	Monaco	**TD**	Tschad
BA	Bosnien-Herzegowina	**GE**	Georgien	**MD**	Republik Moldau	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagaskar	**TJ**	Tadschikistan
BE	Belgien	**GN**	Guinea	**MK**	Die ehemalige jugoslawische Republik Mazedonien	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Griechenland			**TR**	Türkei
BG	Bulgarien	**HU**	Ungarn	**ML**	Mali	**TT**	Trinidad und Tobago
BJ	Benin	**IE**	Irland	**MN**	Mongolei	**UA**	Ukraine
BR	Brasilien	**IL**	Israel	**MR**	Mauretanien	**UG**	Uganda
BY	Belarus	**IS**	Island	**MW**	Malawi	**US**	Vereinigte Staaten von Amerika
CA	Kanada	**IT**	Italien	**MX**	Mexiko		
CF	Zentralafrikanische Republik	**JP**	Japan	**NE**	Niger	**UZ**	Usbekistan
CG	Kongo	**KE**	Kenia	**NL**	Niederlande	**VN**	Vietnam
CH	Schweiz	**KG**	Kirgisistan	**NO**	Norwegen	**YU**	Jugoslawien
CI	Côte d'Ivoire	**KP**	Demokratische Volksrepublik Korea	**NZ**	Neuseeland	**ZW**	Zimbabwe
CM	Kamerun			**PL**	Polen		
CN	China	**KR**	Republik Korea	**PT**	Portugal		
CU	Kuba	**KZ**	Kasachstan	**RO**	Rumänien		
CZ	Tschechische Republik	**LC**	St. Lucia	**RU**	Russische Föderation		
DE	Deutschland	**LI**	Liechtenstein	**SD**	Sudan		
DK	Dänemark	**LK**	Sri Lanka	**SE**	Schweden		
EE	Estland	**LR**	Liberia	**SG**	Singapur		

Verfahren zum digitalen Signieren einer Nachricht

Beschreibung

Die vorliegende Erfindung betrifft ein Verfahren zum digitalen Signieren einer Nachricht sowie die zur Durchführung dieses Verfahrens benötigten Vorrichtungen.

Digitale Signaturen, also elektronische Unterschriften, werden üblicherweise mit Hilfe von sogenannten Public-Key-Verfahren realisiert. Dabei wird einem Signierer ein Schlüsselpaar zugeordnet, das einen geheimen und einen öffentlichen Schlüssel umfaßt. Mittels des geheimen Schlüssels wird durch ein mathematisches Verfahren eine Signatur erzeugt, während mit dem zugehörigen öffentlichen Schlüssel diese Signatur überprüft werden kann. Der geheime Schlüssel steht ausschließlich unter der Kontrolle des Signierers, so daß niemand im Namen des Signierers unterschreiben kann. Der öffentliche Schlüssel hingegen kann veröffentlicht werden, so daß jeder die Signatur prüfen kann. In der Regel wird der geheime Schlüssel über ein Kennwort (PIN) geschützt, so daß zur Durchführung einer Signatur das Wissen über das Kennwort und der Besitz des geheimen Schlüssels notwendig sind.

Digitale Signaturen können in einem Rechner, zum Beispiel in einem PC, mit Hilfe von Software-

Programmen erzeugt werden. Üblicherweise wird dabei der zugehörige geheime Schlüssel auf einer Festplatte oder einer Diskette gespeichert und zur Erzeugung der Signatur in den Hauptspeicher geladen. Meistens wird der geheime Schlüssel selbst wiederum in verschlüsselter Form gespeichert und über ein Kennwort geschützt, welches der Eigentümer beim Signieren über die Software angeben muß. So soll sichergestellt werden, daß nur der Inhaber des geheimen Schlüssels diesen auch zum Signieren verwenden kann. Da keine zusätzliche Hardware benötigt wird, ist dieses Verfahren kostengünstig. Als Nachteil erweist sich, daß sich der Benutzer auf die Integrität der Signatur-Software verlassen muß und diese im allgemeinen als nicht ausreichend sicher angesehen wird.

Als weitere Alternative zur Erzeugung von digitalen Signaturen in einem Rechner dienen Hardwarebasierte Verfahren. Diese verwenden zum Signieren spezialisierte Geräte, bei denen die Darstellungskomponente und die Tastatur per Hardware so mit der Signierkomponente gekoppelt sind, daß auf die Verbindung kein Einfluß genommen werden kann. Diese Geräte werden in der Regel über eine galvanische Verbindung, beispielsweise ein Kabel zur seriellen Schnittstelle, mit dem Rechner verbunden. Diese Geräte verfügen über eine eigene Darstellungskomponente, die die zu signierende Nachricht anzeigt und über eine eigene Tastatur, das sogenannte PIN-Pad, über welche das Kenntwort zum Freischalten des Schlüssels eingegeben wird. Üblicherweise wird der geheime Schlüssel nicht im Signiergerät gespei-

chert, sondern auf einer Chip-Karte, die in das Gerät eingeführt werden kann. Die eigentliche Signatur kann auf der Chip-Karte erzeugt werden (bei Chip-Karten mit eigenem Kryptoprozessor) oder aber im Gerät. Das beschriebene Hardware-basierte Verfahren stellt ein abgeschlossenes Signiersystem aus Darstellungskomponente, Tastatur, Lesegerät und Chip-Karte dar.

Im Unterschied zu den Software-basierten Verfahren sind Hardware-basierte Verfahren erheblich sicherer, wobei jedoch deren Kosten höher sind. Demgemäß werden gegenwärtig sogenannte gemischte Verfahren eingesetzt. Dabei werden die geheimen Schlüssel meistens auf einer Chip-Karte gespeichert und über ein Lesegerät verfügbar gemacht. Die übrigen Aufgaben wie Darstellung, Eingabe des Kennworts und Erzeugung der Signatur erfolgen ganz oder teilweise im Rechner. Dabei kann vorgesehen sein, daß das Signiergerät, das heißt der Leser und die Chip-Karte, als reines Speichermedium für den geheimen Schlüssel verwendet wird, während die Darstellung, die Eingabe des Kennwortes und die Erzeugung der Signatur vollständig im Rechner erzeugt werden.

Alternativ kann vorgesehen sein, die Darstellung und die Eingabe des Kennwortes über den Rechner erfolgen zu lassen, wobei das Signiergerät zusätzlich zur Speicherung des geheimen Schlüssels auch zur Erzeugung der Signatur verwendet wird. Schließlich existiert die Variante, daß nur die Darstellung im Rechner erfolgt. Das Signiergerät verfügt in dieser Variante über eine eigene Tastatur oder ist direkt

mit der Rechner-Tastatur unter Umgehung der Rechner-Software verbunden. Die Signatur wird im Signiergerät erzeugt. Je mehr Aufgaben dabei von der Rechner-Software übernommen werden und je weniger das Signiergerät leisten muß, desto kostengünstiger ist das Verfahren.

Grundsätzlich besteht in all diesen Ausführungsformen jedoch das Problem, daß genau die Daten signiert werden müssen, die der Benutzer signieren möchte. Es muß also ausgeschlossen werden, daß ein Virus beispielsweise die Daten während der Übertragung von der Darstellungskomponente, zum Beispiel dem Display, an die Signierkomponente, zum Beispiel den Kryptoprozessor, verändert. Ferner muß sichergestellt werden, daß eine Geheimzahl (zum Beispiel PIN), die zur Auslösung der Signaturen notwendig ist, nicht von anderen Programmen von der Tastatur mitgelesen werden kann und Dritten bekannt wird.

Zudem wird der möglichst flächendeckende Einsatz der Möglichkeit zur digitalen Signatur durch die vergleichsweise geringe Verbreitung von Signiergeräten eingeschränkt. In potentiellen Anwendungsbereichen digitaler Signaturen, wie beispielsweise dem Internet-Banking, müßte demgemäß eine kostenaufwendige Infrastruktur zur Verbreitung der Signiergeräte geschaffen werden. Problematisch ist dabei auch die Installation von Signiergeräten am Rechner. Einerseits müssen die Geräte physikalisch mit dem Rechner verbunden werden, wobei die seriellen Schnittstellen eines PC häufig bereits belegt sind. Alternative Verfahren zur Anbindung der Si-

gniergeräte an Rechner sind ebenfalls problematisch, da hierfür zumindest die Installation von Software-Treibern und manchmal auch von zusätzlicher Hardware notwendig ist. Zusätzlich müssen für alle Signiergeräte häufig spezielle Software-Komponenten installiert werden, die es dem Anwendungsprogramm erlauben, mit dem Signiergerät zu kommunizieren.

Ein weiteres Problem der herkömmlichen Verfahren zur digitalen Signatur besteht darin, daß diese standortabhängig sind. Bestimmte Anwendungsbereiche für den Einsatz digitaler Signaturen, wie beispielsweise das Internet-Banking, sind aufgrund überall zugänglicher öffentlicher Internet-Terminals standortunabhängig. Würden diese Internet-Banking-Anwendungen nun mit den bekannten standortabhängigen Verfahren zur digitalen Signatur kombiniert werden, wäre die Standortunabhängigkeit dieser Anwendungsbereiche verloren.

Das der vorliegenden Erfindung zugrundeliegende technische Problem besteht also darin, ein kostengünstiges, leicht zu realisierendes und standortunabhängiges Verfahren zum digitalen Signieren von Nachrichten sowie dafür geeignete Vorrichtungen bereitzustellen.

Dieses technische Problem wird durch die Lehre gemäß Hauptanspruch gelöst. Die Erfindung sieht demgemäß ein Verfahren zum digitalen Signieren einer über ein Kommunikationsnetz an ein Signiergerät übertragenen zu signierenden Nachricht vor, wobei

die zu signierende Nachricht mittels eines Telefonnetzes an ein Signiergerät übertragen wird. In besonders bevorzugter Ausführungsform der Erfindung ist das Signiergerät ein Mobilfunktelefon und das Kommunikationsnetz dementsprechend das Mobilfunknetz.

Im Zusammenhang mit der vorliegenden Erfindung wird unter einem digitalen Signieren einer Nachricht ein Vorgang verstanden, bei dem auf elektronischem Wege der Wille zur Abgabe und der Inhalt einer Nachricht bestätigt wird. Dies geschieht durch partielle oder vollständige Verschlüsselung der zu signierenden Nachricht oder durch Verschlüsselung einer kryptographischen Prüfsumme dieser Nachricht in eine signierte Nachricht mittels eines geheimen Schlüssels unter Anwendung eines mathematischen Verfahrens. Im Zusammenhang mit der vorliegenden Erfindung wird unter einer signierten Nachricht entweder die signierte Nachricht als ganze oder die Signatur selbst verstanden. Die Signierung dient dazu, später eine Authentifizierung des Nutzers durchführen zu können. Im Zusammenhang mit der vorliegenden Erfindung wird also unter einer signierten Nachricht auch nur die elektronisch erzeugte Signatur der Nachricht verstanden. Im Zusammenhang mit der vorliegenden Erfindung wird unter einer Nachricht jegliche Art von in elektronischer Form wiedergebbarer Information, beispielweise Zahlen, Buchstaben, Zahlenkombinationen, Buchstabenkombinationen, Grafiken, Tabellen etc. verstanden. Im Zusammenhang mit der vorliegenden Erfindung wird unter einem Signiergerät eine Einheit verstanden, die eine Si-

gnierung einer Nachricht durchführen kann, das heißt einen geheimen Schlüssel, ein mathematisches Verschlüsselungsverfahren, Dialogmöglichkeiten mit dem Signierer oder Nutzer, gegebenenfalls notwendigen Schnittstellen und eine Sende- und Empfangsvorrichtung aufweist. Diese Einheit kann aus verschiedenen Elementen, zum Beispiel aus einer Chip-Karte und einem Lesegerät oder einer Chip-Karte und einem Mobilfunktelefon, aufgebaut sein. Eine Signiervorrichtung ist im Zusammenhang mit der vorliegenden Erfindung eine Komponente des Signiergeräts, die den geheimen Schlüssel und/oder das Verschlüsselungsverfahren und/oder eine Schnittstelle zu beiden oder einer der vorgenannten Komponenten aufweist.

Aufgrund der erfindungsgemäß besonders bevorzugten Verwendung des Funktelefonnetzes zur Übertragung der zu signierenden Nachrichten an ein Signiergerät, das in vorteilhafter Ausgestaltung als Mobilfunktelefon ausgeführt ist, ist es möglich, von einem handelsüblichen Rechner mit Anschluß an einen entsprechenden Nachrichten-Server, zum Beispiel via e-Mail, Nachrichten an das Signiergerät zu übermitteln, ohne am Rechner selbst Installationen oder andere Veränderungen vornehmen zu müssen.

In besonders bevorzugter Ausführungsform sieht die Erfindung ein Verfahren der vorgenannten Art vor, wobei die zu signierende Nachricht von einer auch als Nachrichtenquelle zu bezeichnenden Sendevorrichtung, beispielsweise einem PC, an eine Empfangsvorrichtung, beispielsweise einen Nachrichten-

Server, übertragen wird, anschließend diese Nachricht von der Empfangsvorrichtung an ein der Sendevorrichtung zugeordnetes Signiergerät, insbesondere Mobilfunktelefon übertragen wird, anschließend diese Nachricht im Mobilfunktelefon signiert wird, und sodann an die Empfangsvorrichtung als Signatur, das heißt als signierte Nachricht, zurückübertragen wird.

Die Erfindung sieht also vor, daß von einer Nachrichtenquelle eine unsignierte bzw. zu signierende Nachricht an eine Empfangsvorrichtung, zum Beispiel einen Nachrichten-Server, übertragen wird. Die Empfangsvorrichtung nimmt dann eine Zuordnung der zu signierenden Nachricht zu dem Signiergerät, insbesondere dem Mobiltelefon, vor. Dies geschieht entweder durch eine in der Empfangsvorrichtung hinterlegte Dokumentation oder über Informationen, die zusammen mit der zu signierenden Nachricht von der Sendevorrichtung an die Empfangsvorrichtung übertragen wurde. Die Zuordnung des Signiergeräts, vorteilhafterweise des Mobilfunktelefons, zu der Nachrichtenquelle braucht also keine räumliche Zuordnung zu sein, sondern ist eine rein informatorische Zuordnung. Die Zuordnung besteht also darin, festzustellen, welches Signiergerät und damit welcher Nutzer die empfangene, zu signierende Nachricht signieren soll. Das in bevorzugter Ausführungsform der Erfindung eingesetzte Mobilfunktelefon ist in vorteilhafter Weise in der Lage, eine zu signierende Nachricht darzustellen und auf Anweisung des Nutzers und unter Zuhilfenahme der in vorteilhafter Weise eingesetzten Chip-Karte zu signieren. Die auf

diese Weise signierte Nachricht wird der Empfangsvorrichtung übermittelt und dort gegebenenfalls mit der ursprünglichen Nachricht verglichen und authentifiziert. Von der Empfangsvorrichtung wird die signierte und gegebenenfalls authentifizierte Nachricht dann an einen Adressaten weitervermittelt.

Die Erfindung betrifft auch ein vorgenanntes Verfahren, wobei in vorteilhafter Weise vorgesehen ist, zum Signieren ein Public-Key-Verfahren einzusetzen, bei dem die Sendevorrichtung über einen ihr zugeordneten geheimen Schlüssel und die Empfangsvorrichtung über den entsprechenden, dem geheimen Schlüssel zugeordneten öffentlichen Schlüssel verfügt. Diese Vorgehensweise bietet den Vorteil, daß die Schlüssel nicht übermittelt werden müssen.

In einer weiteren vorteilhaften Ausgestaltung betrifft die Erfindung ein vorgenanntes Verfahren, wobei die zu signierende Nachricht oder die bereits signierte Nachricht, das heißt zum Beispiel die Signatur zwischen Empfangsvorrichtung und Signiergerät, insbesondere Mobilfunktelefon, mittels des Short-Message-Service (SMS) übertragen werden. In besonders bevorzugter Ausführungsform kann vorgesehen sein, daß sowohl die Übertragung der zu signierenden Nachricht von der Empfangsvorrichtung zum Mobilfunktelefon als auch die Übertragung der signierten Nachricht bzw. der Signatur vom Mobilfunktelefon zur Empfangsvorrichtung mittels des SMS durchgeführt wird.

Die Erfindung sieht in einer weiteren Ausführungsform vor, daß die zu signierende Nachricht mittels einer im Mobilfunktelefon vorgesehenen Anzeigeeinrichtung dargestellt wird. Dies kann auf dem Display handelsüblicher Mobilfunktelefone geschehen. Auf diese Weise lassen sich ohne weiteres einfache Texte, wie zum Beispiel Banktransaktionen oder sogar einfache Grafiken, darstellen.

Im Anschluß an diese gegebenenfalls vorgesehene Darstellung gibt der Benutzer in einem dafür vorgesehenen Dialog eine entsprechende Anweisung zur Auslösung des Signierens. In besonders bevorzugter Ausführungsform sieht die Erfindung ein Verfahren der vorgenannten Art vor, wobei der zum Signieren notwendige geheime Schlüssel in einer Chip-Karte des Mobilfunktelefons abgelegt ist und dieser Schlüssel mittels einer über eine Tastatur des Mobilfunktelefons eingebbaren Geheimzahl (im folgenden PIN genannt) freigegeben wird. In vorteilhafter Weise kann durch eine entsprechende übliche Programmierung des Mobilfunktelefons sichergestellt werden, daß die eingegebene PIN nur auf die Chip-Karte übertragen wird und nicht von außen abgehört werden kann.

In einer weiteren alternativen Ausgestaltung der vorgenannten erfindungsgemäßen Verfahren ist vorgesehen, daß der zum Signieren notwendige geheime Schlüssel über eine Tastatur des Mobilfunktelefons eingegeben wird.

In einer weiteren bevorzugten Ausführungsform der Erfindung ist vorgesehen, daß in einem der vorgenannten Verfahren der geheime Schlüssel nicht nur auf der Chip-Karte des Mobilfunktelefons gespeichert ist, sondern dort auch das Signieren der Nachricht durchgeführt wird. Damit kann in vorteilhafter Weise sichergestellt werden, daß der geheime Schlüssel auf keinen Fall die Chip-Karte verläßt und damit von Unbefugten verwendet werden kann.

In einer weiteren vorteilhaften Ausgestaltung der Erfindung ist vorgesehen, daß das Mobilfunktelefon nicht nur zum Signieren der Nachricht, sondern zusätzlich auch als Sender zur Übermittlung der signierten Nachricht an die Empfangsvorrichtung eingesetzt wird.

Die Erfindung betrifft auch Vorrichtungen zur Durchführung der vorgenannten Verfahren, insbesondere Mobilfunktelefone und Chip-Karten.

In einer besonders bevorzugten Ausführungsform der Erfindung ist ein Mobilfunktelefon vorgesehen, das eine Tastatur, eine Anzeigevorrichtung und eine Chip-Karten-Einrichtung zum Lesen und/oder Schreiben einer in das Mobilfunktelefon einsteckbaren Chip-Karte umfaßt, wobei zusätzlich eine Signiervorrichtung vorgesehen ist, die beispielsweise zur Kommunikation mit einer erfindungsgemäßen Chip-Karte und/oder zur Erstellung einer signierten Nachricht aus einer zu signierenden Nachicht geeignet ist. In vorteilhafter Weise ist die Signiervor-

richtung mit der Tastatur zur Eingabe eines geheimen Schlüssels oder einer Geheimzahl verbunden.

In besonders vorteilhafter Ausgestaltung des vorgenannten Mobilfunktelefons ist vorgesehen, daß die Signiervorrichtung eine gegenüber der herkömmlichen Softwarekomponente eines Mobilfunktelefons geänderte Softwarekomponente darstellt. Diese geänderte Softwarekomponente ist in einer bevorzugten Ausgestaltung der Erfindung dazu geeignet, das Signieren der Nachricht nach Dialog mit dem Nutzer durchzuführen. In einer weiteren Ausführungsform ist die erfindungsgemäß vorgesehene geänderte Softwarekomponente des Signiergeräts vorteilhafterweise in der Lage, mit der erfindungsgemäßen Chip-Karte zur Durchführung des erfindungsgemäßen Signierens kommunizieren zu können. In besonders vorteilhafter Ausgestaltung der Erfindung ist vorgesehen, daß die Signiervorrichtung des Signiergeräts zusätzlich Algorithmen abarbeiten kann, die die Anzeige der zu signierenden Nachricht im Anzeigefeld des Mobilfunktelefons ermöglichen.

In besonders vorteilhafter Weise stellt die vorliegende Erfindung also ein System zur Verfügung, gemäß dem lediglich Softwarekomponenten gegenüber in herkömmlicher Weise verwendeter Softwarekomponenten zu modifizieren sind. Eine Änderung der Hardware ist nicht notwendig.

In einer weiteren Ausgestaltung der Erfindung betrifft die Erfindung auch Chip-Karten für Mobilfunktelefone, insbesondere für die vorgenannten Mo-

bilfunktelefone, wobei die Chip-Karte eine Signiervorrichtung umfaßt, die den geheimen Schlüssel des Nutzers speichern kann. In vorteilhafter Weise ist die Signiervorrichtung der Chip-Karte darüber hinaus in der Lage, aus einer vom Mobilfunktelefon empfangenen Nachricht, das heißt einer zu signierenden Nachricht, eine signierte Nachricht zu erstellen. Im Zusammenhang mit der vorliegenden Erfindung wird unter der Signiervorrichtung einer erfindungsgemäßen Chip-Karte also eine Vorrichtung verstanden, die den geheimen Schlüssel des Nutzers speichert, und in vorteilhafter Ausgestaltung auch das Signieren durchführt. Die Durchführung des Signierens muß jedoch nicht unmittelbar auf der Chip-Karte, sondern kann durch eine Software- und/oder Hardwarekomponente im Mobilfunktelefon erfolgen.

Weitere vorteilhafte Ausgestaltungen der Erfindung ergeben sich aus den Unteransprüchen.

Die Erfindung wird anhand der Figuren sowie des dazugehörigen Ausführungsbeispiels näher erläutert.

Die Figuren zeigen:

Figur 1 stellt den Ablauf des erfindungsgemäßen Verfahrens,

Figur 2 in schematischer Weise den Aufbau eines erfindungsgemäßen Mobilfunktelefons und

Figur 3 eine schematische Darstellung einer erfindungsgemäßen Chip-Karte dar.

Die Figur 1 stellt die Sendevorrichtung 1, die in Form eines einen Texteditor oder ein Homebanking-Programm aufweisenden PCs ausgeführt sein kann, eine zu signierende Nachricht 3, eine Empfangsvorrichtung 5, die in Form eines Nachrichten-Servers ausgeführt ist, ein Mobilfunktelefon 7, eine signierte Nachricht 9 und einen Adressaten 11 dar.

Mittels eines in der Sendevorrichtung 1 enthaltenen Homebanking-Programms wird eine zu signierende Nachricht 3, beispielsweise per e-Mail an die Empfangsvorrichtung 5 gesendet. Die Empfangsvorrichtung 5 wandelt die empfangene zu signierende Nachricht 3 in eine Nachricht um, die an das Mobilfunktelefon 7 gesendet werden kann, insbesondere mittels eines Mobilfunknetzes, in vorteilhafter Ausgestaltung mittels des SMS. Die Empfangsvorrichtung 5 ordnet die zu signierende Nachricht 3 dem Mobilfunktelefon 7, beispielsweise mittels einer in der Empfangsvorrichtung 5 hinterlegten Information, zu. Es kann auch vorgesehen sein, daß die Zuordnung mittels einer von der Sendevorrichtung 1 zusammen mit der zu signierenden Nachricht 3 übermittelten Information erfolgt. Bei dieser Information handelt es sich im allgemeinen um die Mobilfunktelefonnummer.

Im Mobilfunktelefon 7 wird die empfangene Nachricht 3 in einer Anzeigeeinrichtung 13 dargestellt. Die genaue Verfahrensweise wird in der Beschreibung zu Figur 2 näher erläutert. Nach Anzeige der zu signierenden Nachricht 3 in der Anzeigeeinrichtung 13

wird die zu signierende Nachricht 3 auf Anweisung des Benutzers signiert und die signierte Nachricht 9 an die Empfangsvorrichtung 5 oder auch an einen anderen Empfänger weitervermittelt. Die Übertragung der signierten Nachricht 9 vom Mobilfunktelefon 7 zur Empfangsvorrichtung 5 geschieht ebenfalls mittels SMS. Die Empfangsvorrichtung 5 kann die signierte Nachricht 9 mit der ursprünglichen zu signierenden Nachricht 3 vergleichen und anschließend an einen Adressaten 11 übermitteln. Die Übermittlung an den Adressaten 11 kann auf beliebigem Wege erfolgen.

Die Figur 2 stellt ein Mobilfunktelefon 7 dar. Das Mobilfunktelefon 7 umfaßt eine Anzeigeeinrichtung 13, eine Sende- und Empfangseinrichtung 15, eine Chip-Karten-Einrichtung 17, eine Tastatureinrichtung 19 und eine Signiervorrichtung 21.

Die von der Empfangsvorrichtung 5 übersandte zu signierende Nachricht 3 wird von der Sende- und Empfangseinrichtung 15 des Mobilfunktelefons 7 empfangen und gegebenenfalls aufbereitet an die Signiervorrichtung 21 weitergeleitet. Die Signiervorrichtung 21 sorgt für die interne Verwaltung des Signaturablaufs. Die Signiervorrichtung 21 enthält Softwarekomponenten zur Ansteuerung der Anzeigeeinrichtung 13, so daß die zu signierende Nachricht 3 visualisiert werden kann. Weiterhin wird die zu signierende Nachricht 3 innerhalb der Signiervorrichtung 21 signiert. Um den Signiervorgang durchführen zu können, muß die Signiervorrichtung 21 mit der Chip-Karten-Einrichtung 17 kommunizieren. Weiterhin

ist es notwendig, daß die Signiervorrichtung 21 über die Tastatureinrichtung 19 entweder den geheimen Schlüssel direkt oder die PIN übermittelt bekommt. Wird über die Tastatureinrichtung 19 vom Benutzer die PIN eingegeben, die in der Regel kürzer ist, also weniger Stellen umfaßt als der geheime Schlüssel, so kann die PIN mittels eines Betriebssystems einer Chip-Karte 25 den unhandlichen geheimen Schlüssel für den Signiervorgang quasi freigeben. Über eine bidirektional ausgelegte Verbindungsleitung 23 kann die Signiervorrichtung 21 mit der Chip-Karte 25 kommunizieren. Die Chip-Karten-Einrichtung 27 trägt dafür Sorge, daß die Befehle oder Kommandos der Signiervorrichtung 21 ausgeführt werden und die signierte Nachricht 9 über die Signiervorrichtung 21 an die Sende- und Empfangseinrichtung 15 weitergegeben wird. Das heißt, die Chip-Karten-Einrichtung 27 stellt eine Schnittstelle zwischen Signiervorrichtung 21 und der Chip-Karte 25 dar.

Die Figur 3 stellt in sehr vereinfachter schematischer Darstellung eine erfindungsgemäße Chip-Karte 25 dar. Diese umfaßt im wesentlichen ein Kontaktierpad 31 sowie eine Speichereinheit 27 und ein Kryptographiemodul 29. In der Speichereinheit 27 ist der für die Erstellung der signierten Nachricht 9 notwendige geheime Schlüssel abgelegt. Das Kryptographiemodul 29 dient der Verschlüsselung der zu signierenden Nachricht 3, beispielsweise mittels eines RSA-Verfahrens. Über das Kontaktierpad 31 kann die Speichereinheit 27 bzw. das Kryptographiemodul 29 mit der Chip-Karten-Einrichtung 27 in kom-

munikativer Verbindung stehen. Aus Gründen der Übersichtlichkeit sind weitere, für den Betrieb der Chip-Karte 25 notwendige Elemente wie beispielsweise ein Controller in der Darstellung der Figur 3 nicht dargestellt.

Ansprüche

1. Verfahren zum digitalen Signieren einer über ein Kommunikationsnetzwerk an ein Signiergerät übertragenen und zu signierenden Nachricht, wobei die zu signierende Nachricht mittels eines Telefonnetzes an das Signiergerät übertragen wird.

2. Verfahren nach Anspruch 1, wobei das Signiergerät ein Mobilfunktelefon ist.

3. Verfahren nach einem der vorhergehenden Ansprüche, wobei die zu signierende Nachricht von einer Sendevorrichtung an eine Empfangsvorrichtung, diese Nachricht anschließend von der Empfangsvorrichtung über ein Telefonnetz, insbesondere ein Mobilfunktelefonnetz, an ein der Sendevorrichtung zugeordnetes Mobilfunktelefon übertragen wird, diese Nachricht sodann im Mobilfunktelefon signiert und an die Empfangsvorrichtung als signierte Nachricht zurückübertragen wird.

4. Verfahren nach einem der vorhergehenden Ansprüche, wobei zur Signierung ein Public-Key-Verfahren

eingesetzt wird, insbesondere ein Public-Key-Verfahren, bei dem die Sendevorrichtung über einen ihr zugeordneten geheimen Schlüssel und die Empfangsvorrichtung über den entsprechenden, dem geheimen Schlüssel zugeordneten öffentlichen Schlüssel verfügt.

5. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Nachrichten zwischen Empfangsvorrichtung und Mobilfunkttelefon mittels des Short-Message-Service (SMS) übertragen werden.

6. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Nachricht vor der Signierung mittels einer im Mobilfunktelefon vorgesehenen Anzeigeeinrichtung dargestellt wird.

7. Verfahren nach einem der vorhergehenden Ansprüche, wobei der zur Signierung notwendige geheime Schlüssel über eine Tastatureinrichtung des Mobilfunktelefons eingegeben wird.

8. Verfahren nach einem der vorhergehenden Ansprüche, wobei der zur Signierung notwendige geheime Schlüssel in einer Chip-Karte des Mobilfunktelefons abgelegt ist, und dieser Schlüssel mittels einer über eine Tastatureinrichtung des Mobilfunktelefons

eingebbaren Geheimzahl (PIN) freigegeben wird.

9. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Chip-Karte die Erstellung der signierten Nachricht durchführt.

10. Verfahren nach einem der vorhergehenden Ansprüche, wobei das Mobilfunktelefon die Erstellung der signierten Nachricht durchführt und wobei der geheime Schlüssel aus der Chip-Karte gelesen wird.

11. Verfahren nach einem der vorhergehenden Ansprüche, wobei das Mobilfunktelefon zusätzlich als Sender zur Übermittlung der signierten Nachricht an die Empfangsvorrichtung dient.

12. Mobilfunktelefon mit einer Tastatur, einer Anzeigevorrichtung und einer Chip-Karten-Einrichtung zum Lesen und/oder Schreiben einer in das Mobilfunktelefon einsteckbaren Chip-Karte, **gekennzeichnet durch** eine Signiervorrichtung (21), insbesondere zur Erstellung einer signierten Nachricht (9) aus einer zu signierenden Nachricht (3) oder/und zur Kommunikation mit einer eine Signiervorrichtung (21) aufweisenden Chip-Karte (25).

13. Mobilfunktelefon nach Anspruch 12, **dadurch gekennzeichnet, daß** die Signiervorrichtung (21) mit

der Tastatureinrichtung (19) zur Eingabe eines geheimen Schlüssels oder einer Geheimzahl verbunden ist.

14. Chip-Karte für ein Mobilfunktelefon, insbesondere nach einem der Ansprüche 12 oder 13, **dadurch gekennzeichnet, daß** die Chip-Karte (25) eine Signiervorrichtung (21) umfaßt, die eine Speichereinheit (27) zur Speicherung des für die Erstellung der signierten Nachricht (9) notwendigen geheimen Schlüssels aufweist.

15. Chip-Karte nach Anspruch 14, **dadurch gekennzeichnet, daß** die Chip-Karte (25) eine Signiervorrichtung (21) umfaßt, die aus einer vom Mobilfunktelefon (7) empfangenen zu signierenden Nachricht (3) eine signierte Nachricht (9) erstellt.

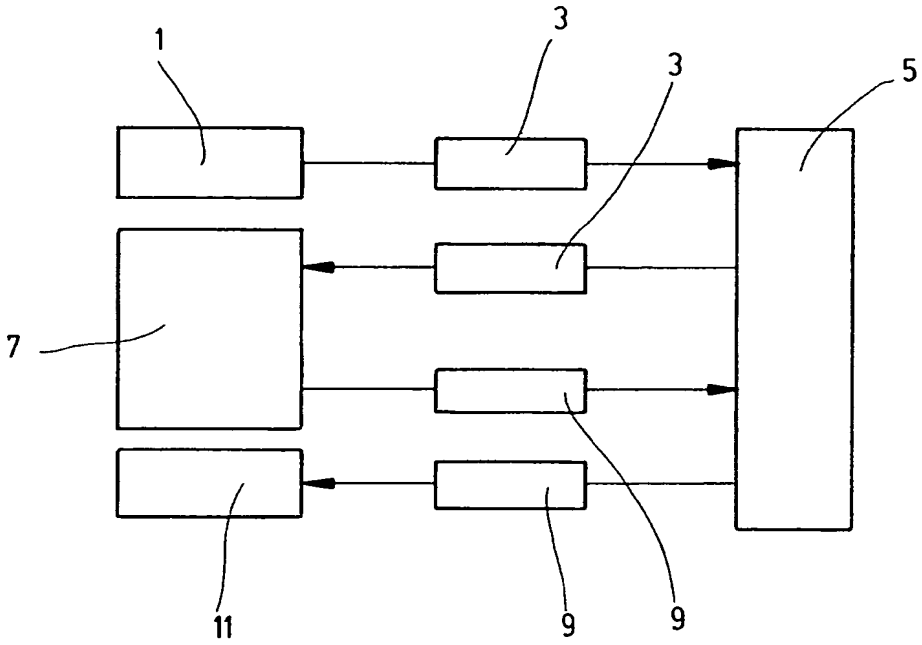


Fig. 1

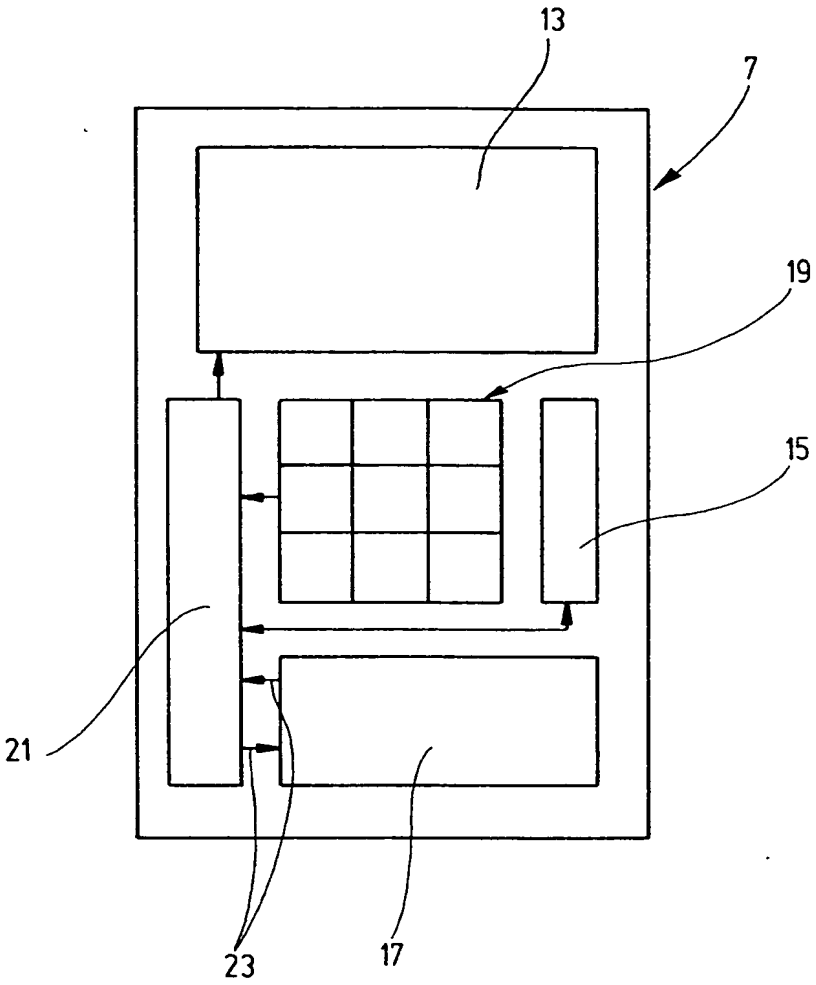


Fig. 2

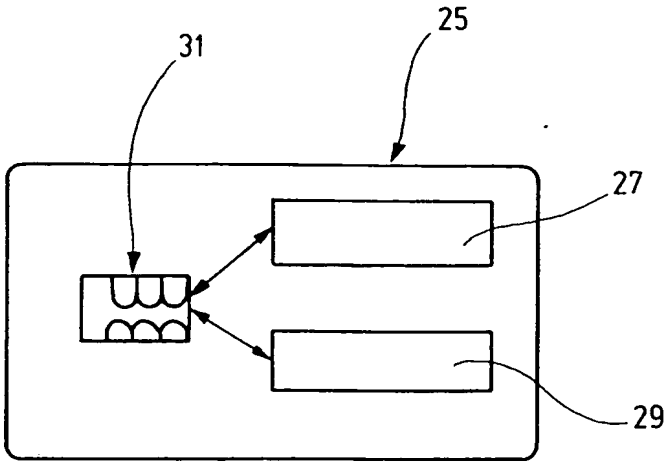


Fig. 3

INTERNATIONAL SEARCH REPORT

Int. tional Application No
PCT/EP 98/06769

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L H04Q G07B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 96 32700 A (AU SYSTEM ;JONSTROEMER ULF (SE)) 17 October 1996 see abstract see page 1-12	1-4,6, 8-15
A	EP 0 689 316 A (AT & T CORP) 27 December 1995 see abstract see column 1, line 56 - column 2, line 28 see column 9, line 4 - line 42 see claim 1 see figures 1,3	1-15

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 March 1999	30/03/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl. Fax: (+31-70) 340-3016	Gautier, L

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Int. .tional Application No
PCT/EP 98/06769

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication.where appropriate, of the relevant passages	Relevant to claim No.
A	COMBANIERE C: "NOUVELLES POSSIBILIT S DE PAIEMENT" REE: REVUE GENERALE DE L ELECTRICITE ET DE L ELECTRONIQUE, no. 4, 1 October 1995, pages 57-65, XP000533330 see the whole document ---	1-15
A	WO 97 37461 A (HEWLETT PACKARD CO ;MAO WENBO (GB)) 9 October 1997 see abstract see page 2, line 23 - page 4, line 25 see page 6, line 23 - page 8, line 15 see claim 1 see figures 1-3 -----	1-15

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int tional Application No
PCT/EP 98/06769

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9632700 A	17-10-1996	SE 506506 C	22-12-1997
		NO 974626 A	13-10-1997
		SE 9501347 A	12-10-1996
EP 0689316 A	27-12-1995	CA 2149067 A	23-12-1995
		JP 8032575 A	02-02-1996
WO 9737461 A	09-10-1997	EP 0891663 A	20-01-1999

INTERNATIONALER RECHERCHENBERICHT

Int. .tionales Aktenzeichen
PCT/EP 98/06769

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 H04L9/32

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 H04L H04Q G07B

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	WO 96 32700 A (AU SYSTEM ;JONSTROEMER ULF (SE)) 17. Oktober 1996 siehe Zusammenfassung siehe Seite 1-12 ---	1-4,6, 8-15
A	EP 0 689 316 A (AT & T CORP) 27. Dezember 1995 siehe Zusammenfassung siehe Spalte 1, Zeile 56 - Spalte 2, Zeile 28 siehe Spalte 9, Zeile 4 - Zeile 42 siehe Anspruch 1 siehe Abbildungen 1,3 --- -/--	1-15

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
23. März 1999	30/03/1999

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Gautier, L

1

INTERNATIONALER RECHERCHENBERICHT

Int. ationales Aktenzeichen
PCT/EP 98/06769

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie	Bezeichnung der Veröffentlichung, soweit erfordertich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	COMBANIERE C: "NOUVELLES POSSIBILIT S DE PAIEMENT" REE: REVUE GENERALE DE L ELECTRICITE ET DE L ELECTRONIQUE, Nr. 4, 1. Oktober 1995, Seiten 57-65, XP000533330 siehe das ganze Dokument	1-15
A	WO 97 37461 A (HEWLETT PACKARD CO ;MAO WENBO (GB)) 9. Oktober 1997 siehe Zusammenfassung siehe Seite 2, Zeile 23 - Seite 4, Zeile 25 siehe Seite 6, Zeile 23 - Seite 8, Zeile 15 siehe Anspruch 1 siehe Abbildungen 1-3	1-15

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Int. ationales Aktenzeichen
PCT/EP 98/06769

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 9632700 A	17-10-1996	SE 506506 C	22-12-1997
		NO 974626 A	13-10-1997
		SE 9501347 A	12-10-1996
EP 0689316 A	27-12-1995	CA 2149067 A	23-12-1995
		JP 8032575 A	02-02-1996
WO 9737461 A	09-10-1997	EP 0891663 A	20-01-1999